UTIOM Framework

Unified Threat-Informed Operations Model Book

Reza Adineh

UTIOM book latest edition

Check out https://UTIOM.de

UTIOM Framework Book
Unified Threat-Informed Operations Model
By: Reza Adineh

Author	Version & Date of release	Description
Reza Adineh	V0.0 2026.02	Initial Version
	V1.0 2026.02	First edition include the examples

Table of Contents

Who this book is for
CISOs, SOC leaders, security architects, detection engineers, IR leaders

How to use it[1]

- Read chapters 1–2 for mindset
- Read 3–6 for implementation
- Use chapter 9 for practical examples

What this book is not
A tool guide, vendor comparison, or compliance checklist.

---

[1] Feel free to reach me out on my LinkedIn. https://www.linkedin.com/in/rezaadineh/

Security operations have reached a defining moment. Across industries, SOCs overflow with alerts and dashboards, yet the people behind them struggle to answer a single question: What is our purpose?

The Unified Threat-Informed Operations Model—UTIOM—is created to answer exactly that.

UTIOM emerged from fifteen years of building and transforming SOCs for banks, FinTech's, and hybrid enterprises. It recognizes that the gap between strategy and execution is the true vulnerability of modern defence. Technology scales quickly; understanding rarely does. UTIOM bridges leadership vision, engineering discipline, and adversary awareness into one coherent, measurable system.

"Security operations are not about collecting logs, running tools and reacting to alerts; they are about understanding intent."

This book presents UTIOM as both a philosophy and a practical framework. It blends management science with detection engineering, providing a roadmap any organization can adapt whether cloud-native or legacy, centralized or distributed.

Introduction

Why UTIOM Exists?

Security operations are at a crossroads.The traditional model focused on isolated monitoring and reactive incident response, no longer meets the demands of today's dynamic threat landscape. Many organizations suffer from fragmented responsibilities, siloed tools, and a lack of cohesion between leadership intent and technical execution.

In practice, this produces predictable failure patterns:

- SOC performance measured by volume (alerts, dashboards, tickets) instead of outcomes
- Detection programs optimized for coverage rather than risk reduction
- Response executed through improvisation instead of engineered playbooks
- Engineering work driven by tools and vendor content rather than crown jewels and threat priorities

UTIOM introduces a holistic, lifecycle-driven model that treats Security Operations and Incident Response as one living system, designed and improved like a product.

What UTIOM Is

UTIOM is an operating model that unifies:

- Leadership direction (vision, governance, accountability)
- Threat-informed strategy (threat profiling, risk prioritization)
- Engineering execution (telemetry, detection-as-code, automation)
- Operational response (playbooks, SOAR, containment discipline)
- Continuous improvement (Kaizen, validation loops, maturity management)

UTIOM is built on widely adopted frameworks such as NIST CSF, TOGAF, MITRE ATT&CK, ISO 27001, and integrates with complementary models like SOC-CMM, plus the author's proprietary frameworks STRATA[2] and TID-CMM[3].

What UTIOM Is Not

UTIOM is not:

- A new compliance framework
- A tool or vendor architecture
- A replacement for NIST CSF, ISO 27001, or SOC-CMM
- A "more detections equals more security" philosophy

UTIOM is a unifying language and lifecycle that helps organizations design security operations that are purpose-driven, threat-informed, and engineering-led.

This Framework introduces a holistic model: The Unified Security Operations Model. It reimagines the entire discipline of cybersecurity operations as one integrated, lifecycle-driven system. The model unifies leadership strategy, software engineering principles, and continuous improvement into a coherent, adaptive process that drives measurable outcomes. Built on top of widely adopted frameworks--NIST CSF, TOGAF, MITRE ATT&CK, ISO 27001--and Author's other proprietary frameworks

---

2 STRATA (Strategy, Talent, Resilience, Automation, Telemetry, Adaptability) is a refined version of People, Process, Technology. It is a new concept I published in LinkedIn.
3 It is a conceptual framework of mine that evaluate Threat Detection Coverage, Detection Engineering, Response & Recovery, Analytics & Automation, Threat Intelligence Integrations & Deception, Governance & Continues Improvement.(for those who are interested, if you followed my works and papers on LinkedIn you can get the idea from my previous published papers.)

STRATA[4] and TID-CMM[5], the model translates theory into practical design. It aligns business value with engineering execution and proposes a universal yet adaptable structure applicable across industries.

The idea of this framework model is simple and it is all about thinking and considering about Security Operation and Incident Resposne as a live system, as a product, and reminding ourself that this is a system desing and this is the way it will work in a meaningful and practical way with expected outcomes, instead of doing separate random operation with no specific goals and siloed way.

If we want to think clearly, and ask a question what is the definition of cyber security and cyber defence? It is actually about Risk control and reducing the Risk, but how it supposed to happen in practic ?
Then the bluprints for operation will come with many different checkboxes. In many companies this is siloed in different teams, different goals, siloed and seperated. There are always gap between Management and Engineering.

If we think clearly we will see the core function of doing all of this, in a practical way is to do the right Security Operation; and Security Operation itself is a system process.[6] The goal of Security Operation is to do the Incident Response in a meaningfull way. That means what we can borrow from NIST to prepare for incidents, have the detection and response capabilities and have a lessones learned form each incident.

But actually comapines needs in practice to be successful in IR and Security Operation, but based on available reports and data[7] from many different sources, (But also from the authors experince) we can see the most companies and busniess they did not think through the Security Operation, They are not mature enough, niether there are no clear vision and plan for imorivement, and in many case they do not have the proper plan, process and people, in some case they spend milion or thousends over different siloed thecnology or buying a service from different vendors, but still they are not satisified or they are far from being effective and preactical in most cases.

NOTE:
There are two main other methodologies that need to be emphasized, the first one is the NIST-CSF, which is actually designed for having a proper Security Operation and, as a result, the right Incident Response, but unfortunately, in my experience, it is not well-received and understood by many companies.
Second is SOC-CMM, which I do like very much, and as a Capability Maturity Model, it could help many Security Operations to have a method and tools to measure specific domains and aspects of a Security Operation, then they would have an idea of their maturity level and their weakness.

Now, let's think one more time, what is a security operation?
Before we can proceed, we need to identify what exactly a security operation. So, a Security Operations with a traditional definition is a function or a unit of People, Processes & Technology to serve the mission of Incident Response for a business.
The core functions would be 4 main functions:
1- Monitoring
2- Detection
3- Analysis
4- Response
5- Prevention
From a structural point of view, there are 3 basic ways to implement it:
1- Internal
2- External[8]
3- Hybrid systems

A model like SOC-CMM helps measure security operations maturity by providing a structured framework to assess a SOC's capabilities and processes across five key domains: Business, People, Process, Technology, and Services. And I highly recommend using it. On the other hand, UTIOM is a framework for businesses and companies to develop their own security operation program in a practical and effective way.

So far, we have seen that Security Operation is a function or unit of operation with a specific goal. So it is the core idea. Basiclay this function is a system, a system that should be applied via an operational unit with a very specific task, to reduce and control risk of cyber threat in real time and increase the readiness of the cybersecurity team.

---

4 STARTA=Strategy, Talent, Resilience, Automation, Telemetry, Adoptability, Evolotion

5 Threat Informed Detection Capability Maturity Model, is still under development.

6 Security Operartion and Incident Response are the same cocepts in practice.

7 Reports like SANS SOC Survey, Splunk State of Security Report, Gurucul "Pulse of AI-Powered SOC" Report, CardinalOps State of SIEM Report, Gartner Magic Quadrant for SIEM, Forrester Wave: Security Analytics Platforms, IBM Cost of a Data Breach Report (The "Gold Standard"), Verizon Data Breach Investigations Report (DBIR), Mandiant M-Trends Report

8 Like MSSPs (Managed Security Service Provider)

Therefore, I used the system design principle, software engineering principal and management principle to develop the UTIOM framework that will help you to implement the security operation in the right way.

So keep in mind that I am trying to bring the best of the other world and put them together to design this framework, so we can rely on them because they are defined models and references.

With all of this in our mind now, we can move forward to the next section to see the foundation of the UTIOM framework.

Terminology and Scope

To avoid ambiguity, UTIOM uses the following definitions:
- Security Operations (SecOps): The overall organizational capability to detect, respond, and continuously reduce cyber risk in operational reality.
- SOC: The organizational function (internal, external, or hybrid) responsible for executing part of SecOps.
- Incident Response (IR): The structured capability to prepare for, detect, analyze, contain, eradicate, recover, and learn from incidents.
- Detection Engineering: The engineering discipline that designs and maintains detection logic, telemetry requirements, testing, and automation as a lifecycle.
- Threat-Informed: Decisions are prioritized based on realistic adversary behaviors and business risk, not generic best practice.

1 The Foundations

Security Operation is like a product and this product need a product designer and a product owner. UTIOM assumes clear ownership of the security operations lifecycle, similar to product ownership in engineering organizations.

1.1 Management and Leadership Principles

"Vision Defines Systems"

Every durable organization begins with a clearly articulated purpose. Let's borrow from Peter Drucker[9]'s principle, "Without a purpose, there is no management," captures the essence of governance. In security operations, vision establishes why the SOC exists, what it protects, and how success is measured. Without it, detection efforts drift toward tool management rather than risk management.

TOGAF[10]'s Architecture Vision and ISO 27001 §5 both mandate top-management direction. UTIOM extends this requirement by treating Vision as the first operational control in the lifecycle. A well-stated vision defines the business value of security, aligns stakeholders, and sets the boundaries for engineering design.

"Strategy as the Bridge"

Henry Mintzberg[11] described strategy as "a pattern in a stream of decisions." UTIOM interprets this to mean that strategy must continually translate high-level objectives into actionable, prioritized outcomes. Where traditional strategies become shelf documents, the UTIOM Strategy domain behaves like a living architecture: capabilities are built, tested, and refined against evolving risk and threat contexts. The bridge between vision and execution remains active.

"Continuous Improvement and Kaizen[12]"

Borrowed from the Toyota Production System, Kaizen emphasizes that small, consistent improvements lead to compound transformation. Deming's PDCA cycle provides the mechanics Plan, Do, Check, Act. In UTIOM, Continuous Improvement is not a trailing activity but an integral feedback phase that restarts the entire lifecycle. Each iteration strengthens strategic clarity, detection precision, and operational confidence.

"Improvement is not a phase; it's a culture."

" Management and leadership role is crucial, therefore we need to select the right methodology"

"Management by Objectives for Defence" Borrowing from Drucker's MBO[13], UTIOM ensures that detection engineers and analysts are not just 'running tools', but are partners in creating value. By setting SMART[14] goals aligned with Crown Jewels protection, the system maintains a 'Spirit of Performance' where every technical action is a traceable step toward a strategic outcome.

Drucker popularized MBO to ensure that everyone in an organization is aligned on shared goals. In a SOC, this prevents "random operation" by ensuring technical tasks serve a strategic purpose.
- Collaborative Goal Setting: Objectives are set through discussion between managers and the technical "knowledge workers" (analysts and engineers), ensuring they understand how their work contributes to the larger vision.
- Cascade of Objectives: High-level strategic goals are translated into day-to-day tasks, such as improving Mean Time to Contain (MTTC) for "Crown Jewel" assets.
- SMART Criteria: Objectives must be Specific, Measurable, Achievable, Realistic, and Time-bound.

"The "Knowledge Worker" as Assets"
Drucker coined the term "knowledge worker" for employees whose primary asset is their theoretical and analytical knowledge.

---

9 Peter Ferdinand Drucker (1909–2005) was an Austrian-American author, educator, and management consultant widely regarded as the "Father of Modern Management". He transformed management into a distinct, teachable discipline that balances technical efficiency with social responsibility.

10 The Open Group Architecture Framework. It is a widely used, open standard methodology and framework for designing, planning, implementing, and governing an enterprise's information technology architecture to align with business goals.

11 Henry Mintzberg is a prominent Canadian academic, author, and Professor of Management Studies at McGill University, known for his influential work in business and management that often challenges conventional wisdom. He has written over 150 articles and more than 20 books on topics including strategy, organizational design, and leadership education.

12 Kaizen (改善) is a Japanese term and business philosophy that means "continuous improvement". The word is composed of two characters: "kai" (meaning change) and "zen" (meaning good). The philosophy centers on the idea that many small, incremental changes made consistently over time can lead to significant positive results in efficiency, quality, and productivity.

13 Management by Objectives

14 Specific, Measurable, Achievable, Realistic, and Time-bound

- Empowerment and Autonomy: Because SOC analysts often know more about specific threats than their managers, they require autonomy to solve unique problems.
- Continuous Learning: Knowledge is "perishable"; it must be constantly improved and challenged, or it vanishes.
- Focus on Strengths: Effective management makes an employee's strengths productive and their weaknesses irrelevant.

"Systematic Abandonment" As Drucker noted, 'If you want something new, you have to stop doing something old'. UTIOM integrates this by treating the pruning of obsolete telemetry and detections as a core engineering discipline, preventing the SOC from becoming a 'factory of data'.

"Be aware of 'Effectiveness vs. Efficiency'"
A core Drucker principle is distinguishing between "doing things right" (efficiency) and "doing the right things" (effectiveness).
- Prioritizing Impact: There is nothing so useless as doing efficiently that which should not be done at all. In UTIOM terms, efficiently detecting "random noise" is a failure of management if it doesn't control actual business risk.
- Measuring Outcomes: Focus on metrics that prove effectiveness (e.g., Risk Reduction) rather than just efficiency (e.g., Number of Alerts).

In fact we should think this way:
- "Vision as the Primary Control": Following Drucker's principle that "Purpose is the starting point of management," UTIOM treats the Vision not as a statement, but as the first operational control that dictates the boundaries of all engineering efforts.
- "The Knowledge Worker's Autonomy": In a UTIOM-led SOC, analysts are "Knowledge Workers" whose primary task is to interpret intent, not just operate or manage tools. Management's role is to provide the "Strategy Bridge" so these workers can exercise "Self-Control" through observability. Management should lead all roles to be aware of the operation model in Security Operation and everyone must be aligned and aware of priorities. (The goal is to be Threat-Informed and it wont achieve until everyone would be on the same page.)
- "Systematic Abandonment": To prevent the "factory of data" from becoming bloated, UTIOM adopts Drucker's rule of "abandoning yesterday." Every Continuous Improvement cycle (Section 2.7) must include a review to "slough off" detection rules that no longer protect a Crown Jewel or address a current threat.
- "Effectiveness over Efficiency": Drucker noted that "Efficiency is doing things right; Effectiveness is doing the right things." UTIOM ensures effectiveness by forcing detection rules to be mapped to a specific risk requirement rather than just high-volume research.

1.2 Engineering and Systems Thinking

SOCs often resemble factories of data rather than engineered systems. They assemble technologies like SIEM, EDR, SOAR without a unifying design logic. UTIOM applies systems engineering to security operations: define inputs, outputs, boundaries, and feedback before integrating components.

"Systems Are Engineered, Not Assembled"
From NASA's engineering philosophy: reliability results from design, not accumulation. UTIOM adopts this by mapping every operational process to its dependencies and feedback signals. For example, telemetry inputs (visibility) produce detection artifacts (outputs) that trigger response mechanisms; response data then feeds the next design cycle.

"DevOps Logic[15] for Detection"[16]
Modern engineering thrives on iteration and testing. UTIOM's detection engineering domain mirrors software practices:
- Test-Driven Detection rules must be verifiable against simulated threats.
- CI/CD Pipelines deploy, validate, roll back safely.
- Version Control trace every rule's lineage and purpose.
- Observability measure false-positive rates, detection coverage, and rule latency.

By codifying detection as engineering code, UTIOM transforms threat detection from reactive art to accountable science.[17]

"Detection becomes engineering, not improvisation."
"UTIOM standardizes the lifecycle and engineering discipline, not the threats or detections themselves."

Note:
Beyond just using Git and CI/CD, apply actual software architecture patterns to how you write detections.
- DRY Principle[18] (Don't Repeat Yourself): move repeated logic and exclusions to shared configuration objects. For example, instead of writing the same IP exclusion list into 50 different SIEM rules, move that list into a global "Configuration Object."
- Abstraction Layers: Create a "Common Information Model", so logic survives vendor changes. Your detection logic should not care if the data comes from CrowdStrike, SentinelOne, or Sysmon. The logic should sit on top of a standardized schema.
- Unit vs. Integration Testing: unit tests, integration tests, and effectiveness tests
  - Unit Testing: Testing a single detection rule against a small JSON log snippet.
  - Integration Testing: Testing how that rule interacts with the alerting pipeline and the SOAR playbook.
  - Effectuality Testing: Testing if the rule would trigger in expected situation.

Borrowed from Industrial Design: Cognitive Ergonomics and "Affordance"
In industrial design, a well-designed tool "tells" you how to use it and it is purpose driven. So a Security Operation should be designed in the same way. Security operations must be designed for human cognition:

- Signal-to-Noise Ratio (SNR) Optimization: Industrial designers remove clutter to focus the user on the primary control. Optimize signal-to-noise ratio through grouping and narrative incidents.
- Standardized Interfaces: Ensure that regardless of the tool, the "Output" (the alert) always follows the same visual hierarchy: What happened? Why does it matter? What is the first step to fix it? And so on. We need the whole story, the big picture, the time-line, not random single alerts.
- Reducing "Alert Fatigue" as a Design Goal: Treat alert fatigue and analyst burnout not as a HR issue, as a system design failure.

"Resilience and Graceful Degradation"
Assume components fail. Security operations must remain functional when sensors are bypassed or degraded:
- Redundant visibility paths (e.g. identity and network telemetry as backup to endpoint)
- Backpressure and circuit breakers for log spikes
- Meta-detections that monitor the health of telemetry and detection pipelines

---

15 Detection Engineering Life Cycle" (DELC)

16 Do not relay on defult detection rules in place, tailore them to your environment. (Even if the default rule looks good for you, you still need to keep them updated regularly.)

17 In case you are not ready to implement the codified system for detection development, do not skip this, it is more about the concept and idea of how to develop a detection code in a managed controlled way like we do release a stable software. For start consider any methodology to develop a code and having a version control for it, and being able to trace a detection for the whole lifecycle of it.

18 The DRY principle is a fundamental software development guideline introduced by Andy Hunt and Dave Thomas in their 1999 book The Pragmatic Programmer. The core idea is that every piece of knowledge, logic, or data within a system should have a single, unambiguous, and authoritative representation.

"Less, But Better: The Minimalism of Defense" Following Dieter Rams[19]' principle that 'Good design is as little design as possible,' UTIOM rejects the accumulation of tools, logs and running different sperate teams and process. Instead, it focuses on the 'Honesty' of detection—ensuring that every alert accurately reflects a business risk and provides an 'Understandable' path to response. By prioritizing 'Unobtrusive' systems that only signal when necessary, we eliminate the noise of the 'data factory' and protect the analyst's cognitive ergonomics. We should design a unified system that works purposefully.

"Feedback Loops as Learning Systems"
Every SOC event true positive, false positive, near-miss becomes structured feedback. Data from detection and response flows back into telemetry design and strategic planning. This creates a self-correcting ecosystem capable of continuous adaptation without external audits.
"Design, don't assemble. Detection should be built with purpose, not patched with panic."

"Systems Engineering: Requirements Traceability (The V-Model)[20]"[i]
Systems engineering dictates that a system's success is measured by how well it meets specific requirements. In many SOCs, detections are added randomly based on "cool" research rather than system needs.
- Requirements Mapping: Every detection artifact should be traced back to a specific risk or threat model (e.g., MITRE ATT&CK). If a detection doesn't map to a requirement, it is usually "waste" in the system.
- Verification vs. Validation:
    o Verification: Does the rule work as intended? (e.g., Does the regex match the log?)
    o Validation: Does the rule actually stop the business risk? (e.g., Does it catch the actual attacker? Or it is just a random prebuilt rule with no risk assigned?)

1.3 The Convergence

Leadership provides direction and intent; engineering provides precision and reliable execution. When disconnected, organizations experience strategic confusion above and operational fatigue below. That is a common point of failure.
UTIOM unifies them through a recursive lifecycle that binds strategy, engineering, and intelligence.

So before we see the schematic concept in a high level diagram, let's recap the idea of UTIOM:
We typically have 3 main pillar for running a Security Operation:
1- Leadership & Governance
2- Engineering & Enablement
3- Operations & Analysis
And each one of them having their own subprocess. In zoom-out we will have the Unified Threat Informed Operation Model. UTIOM provides the unified loop that keeps these pillars aligned through continuous feedback.

For implementing UTIOM we do need to define our Security Operation Vision, with a defined Vision we can now define our Security Operation Strategy, and with a Risk-Based approach we can review our assets and define our Crown-jewels, this can lead to check our visibility of our critical assets and continues development of threat detection rules for them, having detection rules can led to developing proper response plan/playbooks.

The Unified Loop:

---

19 Dieter Rams is a highly influential German industrial designer. He is best known for his long tenure as the head of design for the consumer electronics company Braun from 1961 to 1995, and for his work with the furniture company Vitsœ. His design philosophy, encapsulated by the phrase "less, but better" (Weniger, aber besser), has had a lasting impact on 20th-century aesthetics and modern design practices, notably influencing designers at Apple, such as Jony Ive.

20 V-Model, a structured approach used primarily in software development and systems engineering. The V-Model is a procedural model that visually demonstrates the relationship between each stage of the development life cycle and its corresponding testing phase, which creates the "V" shape.
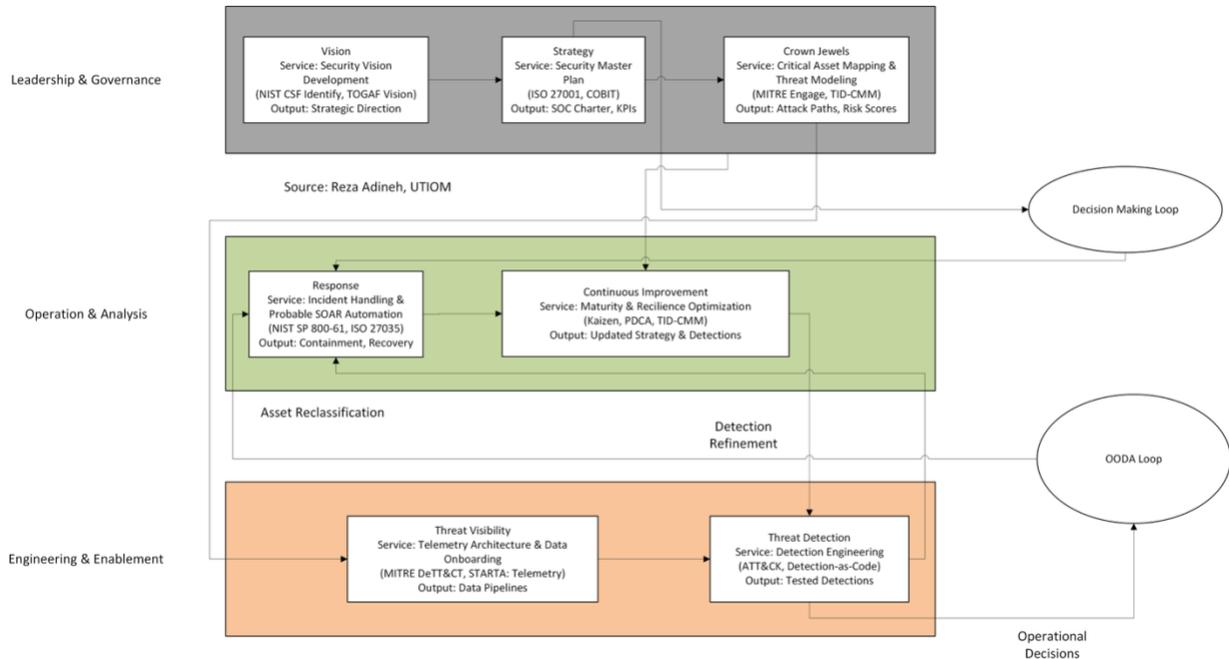
Figure 1- UTIOM high level

Each phase consumes and produces knowledge. Outputs of one become inputs to the next. This cyclical logic converts fragmented operations into an adaptive control system.

Why Unification Matters?

- Strategic Traceability: executives can trace any incident to a policy, metric, or capability.
- Engineering Efficiency: teams build only what serves defined business and threat priorities.
- Cultural Alignment: analysts understand purpose; leaders understand constraints.

The convergence yields a system that learns both top-down and bottom-up a Threat-Informed Organization rather than a reactive monitoring centre.

"A SOC without a vision is an alert factory."

1.4 UTIOM Concept review

A well-defined vision and strategy function like a north star. In Security Operation without defining vision and strategy and knowing the crown jewels it is not possible to accomplish anything successful.

In this section we will see how this UTIOM framework will help you to unified a meaningful threat informed detection and response in a practical way.

Starting with vision, a practical way of defining vision would be defining a meaningful goal, like we are aware of all critical Risk that target our Crown Jewels.

From strategic point of view we need to define at least some basic strategies but practical, doing a threat profiling for our business is one mandatory thing and is the main basic step, that should define the baseline for threat detection approaches. While we knew about our adversaries, their intent, motivation and their probable capabilities, now we can be ready for defend, and align our detection and response program accordingly.

So in summary, UTIOM's practical sequence:

- Define vision for Security Operation, (Vision is why or the target destination, is the goal of the SecOps)
- Define, develop and implement strategy for Security Operation, The main basic activity is about Implementing Threat Profiling and Risk prioritization. (Vision define strategy, Strategy is how to achieve to the defined Vision, it is the practical, logical actionable roadmap to use the vison and implement our Desing.)

- Identifying business key assets & crown jewels, Providing Threat Visibility, (Threat Detection should be an ongoing continues process, and it is fed by Threat modelling and threat intelligence mainly) and model realistic threats against them.
  - Developing aligned Threat Modelling,
  - Checking the visibility status by being sure we generate and collect main necessary telemetry,
  - Considering implementation of deception solutions (In a more mature situation placement of deception solution for a proactive detection and analysis),
- Engineer visibility, ensure telemetry exists where it matters most
- Engineer detection as a lifecycle (code, testing, fidelity, coverage)
- Engineer response via playbooks and automation aligned to threats and crown jewels
- Continuously improve using lessons learned and validation loops (purple team)[ii]

Important note:
Mapping UTIOM to NIST Incident Response

This framework is exactly aligned with Incident Response steps and is a way to modernize, extend and implement the Incident Response for Security Operation in a Threat Informed Way and Risk aware approaches.

In NIST SP 800-61(NIST Incident Response Guidance) phases guideline for Cybersecurity we have 4 main Function/steps:
1- Preparation
2- Detection & Analysis
3- Containment, Eradication & Recovery
4- Post Incident Activity

So to map it with UTIOM it is as below:[iii]

NIST Incident Response Functions	Unified Threat Informed Operation Model (UTIOM) Functions
Preparation	Vision, Strategy, CJ, Threat Profiling, Threat modelling, Threat Visibility
Detection & Analysis	Threat Detection Engineering (rules, tuning, analysis workflows)
Containment, Eradication & Recovery	Response (playbooks, containment automation, recovery coordination)
Post Incident Activity	Continues Improvement(learning loop, updates to strategy and engineering)

In the next section we will explain the Unified Lifecycle that UTIOM farmwork provide for an effective modern and unified way of implementing Incident Response for a Security Operations.

2   The Unified Lifecycle

Security operations become effective only when they are cyclical, not linear. UTIOM defines seven connected domains that together describe the full life of defence and Threat Informed Incident Response.
Each domain is:
- A decision space
- A feedback loop
- A measurable capability[21]

First missing point in many organization is not having the right vision for their Cyber Security Operation or their Risk management. Defining the Vision must lead to define the right strategy. And the strategy should be aligned with the business/company Crown Jewels[22,] and knowing the business critical assets (Crown Jewels)[23],iv will provide the threat visibility through threat modelling, and with having threat visibility we can continuously develop meaningful, aligned threat detection rules that actually matters, not random detection from different source that has nothing to do about our real world cyber risk. While we know what we are looking to detect, then we can develop our response plan based on that and at the final phase of this process we will have a Continuous Improvement to revise and use the lessons learned.

---

[21] Mainly qualitatvie, some quantitavie
[22] Each role in a security Operation must be aware of their operational vission and mission, and this vision and missison are defined based on business operational critical assets.
[23] It is super crucial for defence team to know the CJs, check the endnotes for more details.

2.1 Vision Defining Purpose

While we considers Security Operations as a engineered system we must define how this system would be successful. All engineered systems begin with purpose. In SecOps, purpose answers why we defend and what success means. Without it, SOCs default to counting alerts instead of outcomes.

Core Activities
- Define the business intent of the SOC.
- Align Security Operation Vision with Business CJs.
- Establish governance and accountability.
- Identify success metrics (e.g., availability, confidentiality, safety, continuity).

Outputs
- Long Term and short Term Security Operation Vision.
- Vision statement and policy charter.
- Stakeholder map and alignment workshop results.
- Baseline metrics (e.g., detection confidence, time-to-resolution).

Referenced Frameworks
- TOGAF Vision
- ISO 27001 §5
- NIST CSF (ID.GV).

"Vision is the compass; tools are merely instruments."

2.2 Strategy Translating Vision into Design

Vision without strategy is intention without motion. UTIOM views strategy as a capability-building system rather than a document. Every decision must connect a risk to a measurable improvement.

Core Activities
- Threat and risk prioritization. (Threat Profiling[24] as a core function).
- Resource planning and capability road-mapping.
- Defining measurable KPIs and KRIs tied to crown jewels.

Outputs
- SOC Master Plan and quarterly objectives.
- Threat profile and prioritization model.
- Capability increment schedule.
- Stakeholder scorecards.

Referenced Frameworks
- COBIT Governance.
- ISO 27001 Clauses 6–8
- STRATA[v] Strategy.
- TID-CMM[vi] Strategic Alignment.

2.3 Crown Jewels Focusing on What Matters

No organization can protect everything equally. Crown Jewel Analysis (CJA) identifies critical assets, processes, and data whose compromise would create disproportionate damage.

Core Activities
- Asset inventory and classification.
- Mapping Threat profile with CJ.
- Business impact mapping.
- Threat modelling for identified Crown Jewel (CJ).
- Critical Asset mapping to the high risk Threats.

---

[24] Threat profiling is a proactive cybersecurity process that involves identifying, analyzing, and documenting the specific, relevant adversaries and threats targeting an organization. (https://www.linkedin.com/pulse/cyber-threat-profiling-understanding-different-actors-reza-adineh/?trackingId=NkWFdbDGToWs8KNuWh51Rw%3D%3D), (https://www.linkedin.com/pulse/crowdstrike-mandiant-red-canary-reza-adineh-qrcgf/)

Outputs
- CJ registry with owners.
- Threat profile mapped with CJ and defined high priority TTPs.
- Attack-path diagrams for CJs.
- Checklist of Protection, Detection, Visibility and Response capability readiness for CJs based on top priority TTPs.
- Mapped related MITRE ATT&CK TTP with CJs.
- Dependency matrix linking CJ to data sources.
- Threat Detection rules logic.

Referenced Frameworks
- NIST IR 8183
- MITRE Engage
- ISO 27001 §8
- TID-CMM Threat Prioritization.

"You can't build meaningful visibility without knowing what deserves to be seen."

2.4 Threat Visibility Engineering Telemetry

Visibility is the bloodstream of detection. UTIOM designs visibility from the CJs outward, ensuring telemetry covers what matters first.

Core Activities
- Map ATT&CK tactics to data sources.[25]
- Map Threat Modelling to data sources.[26]
- Define logging and retention standards.
- Define logging, retention, and access standards.
- Implement data quality and normalization checks.
- Implementation of Deception variation aligned with CJ.[27]

Outputs
- Visibility Blueprint and Gap Report.
- Mapped Threat models to required data sources.
- Telemetry onboarding roadmap. (Defined required data pipeline for CJs high priority Threats)
- Threat Activity visibility.
- Metrics: % CJ coverage per Threat, log quality index.

Referenced Frameworks
- NIST SP 800-137
- MITRE DeTT&CT
- CIS Controls v8
- STRATA Telemetry

2.5 Threat Detection Engineering Awareness

You can't detect what you can't observe, but observation without interpretation is noise. Detection must be engineered, version-controlled, and threat-informed.

Core Activities
- Develop Detection rules referenced by Thread modelling in previous steps.
- Develop rules mapped to ATT&CK TTPs.
- Apply Detection-as-Code practices (Git, CI/CD, testing).
- Measure fidelity, coverage, and operational cost.
- Automate QA and regression testing.
- Red/Purple Teaming planning for Detection Verifications.

Outputs
- Detection Repository with traceability.

---

[25] Means those TTPS which are mapped to CJs.

[26] We can leverage Threat-Informed Detection Capability Maturity Model in this activity.

[27] Deploy deception selectively where it increases adversary cost.

- QA Reports with coverage metrics.
  - % of implemented and tuned detection rules per Threat Modelled
  - % of implemented deception in each operational zone
- False positive and false negative monitoring.
- Mean Time to Detect (MTTD) evaluation based on top TTPs.

Referenced Frameworks
- MITRE ATT&CK v18
- DeTT&CT
- Sigma
- STRATA Automation.
- TID-CMM Detection QA.

"Detection built from behaviours lasts longer than detection built from indicators."

2.6 Response Executing with Precision

Response is the natural continuation of detection. UTIOM positions incident handling as an engineered workflow, not an improvisation.

Core Activities
- Developing Response plan, Playbooks aligned with defined Threats.(prioritized threats and crown jewels)
- Automate containment through SOAR.(In case of absence of SOAR, consider containment plan without SOAR)
- Define escalation paths[28] and CJ-specific playbooks.
- Track MTTR, MTTC and containment SLA.

Outputs
- Playbook Library and Response Matrix.
- Incident Records with contextual tags.
- Lessons Learned Repository.

Referenced Frameworks
- NIST SP 800-61
- ISO 27035
- FIRST CSIRT
- STRATA Resilience
- TID-CMM Process Execution.

2.7 Continuous Improvement Learning Systems

No design remains optimal forever. Continuous Improvement is the intelligence loop that converts experience into new strategy.

Core Activities
- Post-incident reviews and Kaizen sessions.
- Red/Purple team validation of detection coverage.
- Update threat models and roadmaps.
- Conduct periodic benchmarking and maturity assessments.

Outputs
- Updated Vision and Strategy documents.
- Proper aligned input for protection, Detection and Response.
- Action plans with owners and timelines.
- Maturity scorecards (UTIOM / TID-CMM / SOC-CMM).

Referenced Frameworks
- Deming PDCA
- Kaizen
- SOC-CMM
- STRATA Adaptability.
- TID-CMM Feedback.

"Learning is the final deliverable of every incident."

---

[28] And decision gates.

3 Capability Layer Model

UTIOM operates across three mutually reinforcing planes. Each layer represents both a technical depth and an organizational perspective.

Layer/Pillar	Focus	Main Goal	Primary Activities	Key Frameworks
Foundational (Leadership & Governance)	1. Vision, 2. Strategy, Missions, 3. Operations Model, 4. Governance, Architecture,	• Know The related Threat • Know yourself	Strategic planning, Role definition, Threat Profiling, Risk alignment	NIST CSF (Identify), ISO 27001, TOGAF
Operational & Analysis	1. Telemetry, 2. Visibility 3. Detection, 4. Analysis, 5. Response, 6. Feedback & Optimization	• Analysis & Response	Threat modelling, Log onboarding, Analysis, SIEM/EDR operations, playbook execution	ATT&CK, ISO 27035, STRATA Resilience
Engineering & Enablement	1. Protection, 2. Visibility, 3. Detection, Automation & QA, 4. Feedback & Optimization	• Build Detection Rules • Build Response Plan	Detection-as-Code, CI/CD, purple team validation, Kaizen loops, hunting, benchmarking	GitOps, DeTT&CT, TID-CMM Detection QA, SOC-CMM, PDCA, STRATA Adaptability

"Layers aren't hierarchies they are symbiotic perspectives."

4 Standards and Framework Integration

UTIOM deliberately aligns to recognized global standards to ensure traceability and compliance of a security operation running a complete incident response process. UTIOM tries to provides traceability between business intent and operational execution.

UTIOM Domains	NIST CSF	ISO 27001 : 2022	Other Frameworks	Description
Vision	Identify (ID.GV)	Clause 5	TOGAF Vision	Executive intent and governance
Strategy	Identify / Protect	Clauses 6-8	COBIT Governance / STRATA Strategy	Converts vision into tactical risk plans, Risk and threat prioritization
Crown Jewels	Identify (ID.AM)	Clause 8	NIST IR 8183 / MITRE Engage	Asset criticality and impact, Threat prioritization
Threat Visibility	Detect (DE.AE)	Annex A 12	DeTT&CT / CIS Controls v8	Telemetry design and data coverage, Threat Modelling
Threat Detection	Detect (DE.CM)	Annex A 12	ATT&CK / Sigma / STRATA Automation	Detection engineering and QA Deception for Detection
Response	Respond (RS)	Annex A 16	NIST 800-61 / FIRST CSIRT / STRATA Resilience	Incident containment and playbooks
Continuous Improvement	Recover (RC)	Annex A 10	SOC-CMM / Kaizen / STRATA Adaptability	Feedback, Learning and maturity management

5 Threat-Informed Maturity Model

UTIOM's maturity ladder measures integration, threat realism, and engineering discipline.

Level	Designation	Characteristics	Threat-Informed Capability	Outcome
0	Absent	Fragmented ownership, Weak Visibility	None	Chaos, alert fatigue
1	Reactive / Threat-Aware	Initial ATT&CK-aligned detections around CJs	Awareness	Context replaces noise
2	Structured / Threat-Informed	CJ-based visibility & versioned rules + Aligned TI[29]	Intentional Design	Predictable defence
3	Integrated / Unified	Feedback ↔ Detection ↔ Strategy linked	Collaboration	Traceable operations
4	Adaptive / Engineering-Led	CI/CD + Purple Team loops	Automation	Rapid iteration & QA
5	Autonomous / Threat-Informed Automation	SOAR + Deception + Continuous Red/Purple teaming and validation	Intelligence	Self-optimizing SOC

Each level builds both vertical (maturity) and horizontal (unification) growth.
Level 5 is aspirational and depends on business risk tolerance, automation safety, and organizational maturity.

---

[29] Threat Intelligence

6 Implementation Blueprint

Implementation follows five progressive phases, each self-validating through metrics.

Phase	Core Actions	Main Deliverables
1- Strategic Alignment	Define vision & governance, Conduct CJ analysis, Threat Profiling and prioritization, Map threats to business risk	• Security Master Plan • Operation Model • Vision Statement • CJs profiles • Measurement Framework • Threat Profiles
2- Visibility Architecture	Threat modelling, Map CJ attack paths to data sources, build telemetry pipeline,	• Threat Models • Visibility Matrix • Gap Analysis • Data Quality KPIs
3- Detection Engineering	Build Detection-as-Code pipeline, apply CI/CD, QA tests, Providing required data feed for detection	• Detection Repository • QA Reports • Coverage Metrics
4- Response Execution	Deploy Response playbooks, Deploy SOAR playbooks, measure MTTR, refine containment flows	• Playbook Catalog • Incident KPIs
5- Feedback & Evolution	Kaizen reviews, Red/Purple team validation, update strategic roadmap	• Updated KPI • Dashboard Maturity Benchmark • Detection assessment and verification reports

"Implementation is a journey of validation, not deployment."

6.1 Mapping Security Operations Processes to UTIOM

Common Traditional SOC Process	How It's Commonly Treated	UTIOM Interpretation	UTIOM Lifecycle Anchor
Threat Intelligence	Separate upstream function	Incident Response before impact, shaping assumptions and priorities	Strategy → Crown Jewels
Threat Modeling	If even exist. Design-time exercise	Incident Response planning against likely adversaries. (Unifeid and integrated Detection & Response)	Strategy → Threat Visibility
Detection Engineering	If even exist. Technical rule-writing task	Incident Response encoded into logic and telemetry. Detection is purposful and a live operating system. High fidelity detection rules compare to random deufult detection tules.	Threat Detection Engineering
Threat Hunting	Proactive activity outside IR	Incident Response without alerts, hypothesis-driven. Purposful.	Threat Detection → Response
Monitoring & Alerting	Firefighting approches usually. Real-time alert handling	Continuous low-intensity Incident Response. Monitoring for what matters most. Knwoing the prority and Threat Informed monitoring & alerting.	Threat Detection

Common Traditional SOC Process	How It's Commonly Treated	UTIOM Interpretation	UTIOM Lifecycle Anchor
Alert Triage	Firefighting approches usually. Noise reduction steps if possible.	Decision refinement inside Incident Response. Threat Informed Detection aligned with Response readiness.	Response
Incident Investigation	Core IR activity	Strategic awareness. High-intensity Incident Response in highest matured implementation.	Response
Containment & Eradication	Separated Process. Usually ditributed between different teams. Firefighting approches. Reactive technical action.	Pre-designed Incident Response execution. The Response is mature and predefind and aligned with Threat Detection. Reponse is a part of a living operating system.	Response → Resilience
Forensics	Post-incident activity. Usually lack of required data.	Incident Response validation and learning. It is part of live operating system after incident.	Continuous Improvement
Lessons Learned	Optional retrospective	Incident Response feedback loop. It is a part of live operating system. It is ongoing process and it is not just restricted to an optional retrospective after an incident.	Continuous Improvement
Metrics & Reporting	Management overhead	Incident Response health indicators	Vision → Strategy
Training & Exercises	Separate readiness program. (If it exist at all)	Incident Response rehearsal	Resilience & Adaptability

Mapping Common IR phase from SANS and NIST model to UTIOM:

UTIOM Lifecycle Stage	SANS IR Phase(s)	NIST IR Phase(s)	What it means in UTIOM (modern, realistic)	Key capabilities (explicit)
Vision	Preparation	Preparation	Define purpose, success criteria, decision authority, and resilience outcomes tied to business services.	Impact tolerance, crisis posture, comms principles
Strategy	Preparation	Preparation	Translate vision into priorities, operating model, measurable outcomes, and investment focus.	Coverage goals, SOC-as-product cadence, metrics/SLOs
Crown Jewels	Preparation	Preparation	Identify critical services, data, identities, and trust boundaries; define what must not fail.	Service tiering, identity crown jewels, dependencies
Threat Modeling	Preparation	Preparation	Model likely adversaries, paths, and abuse cases against crown jewels; define "detection stories" and response intent.	Threat scenarios, ATT&CK technique selection, kill-chain paths, misuse cases, assumptions, crown-jewel attack paths
Threat Visibility Engineering	Preparation	Preparation	Engineer telemetry and evidence pipelines across endpoint/identity/network/cloud to support the modeled threat paths.	Logging design, enrichment, evidence readiness, deception sensors wiring
Threat Detection Engineering	Preparation (+ readiness)	Preparation (+ readiness)	Build detections as engineered artifacts aligned to modeled behaviors and telemetry reality; define tuning/acceptance.	Rule lifecycle, test cases, purple teaming validation, detection SLOs
Threat Detection Operations	Identification	Detection & Analysis	Continuous sensing, triage, enrichment, validation, and scoping decisions.	Entity timelines, investigation playbooks, intel-as-context
Threat Hunting	Identification (proactive)	Detection & Analysis (proactive)	Hypothesis-led hunts derived from threat models and visibility gaps; feeds detection backlog.	Hunt library, gap-driven hunts, campaign hunts
Response	Containment, Eradication, Recovery	Containment/Eradication/Recovery	Execute containment, eradication, and recovery with clear authority, playbooks, and business-aware actions. Fully aligned with threat detection that already covers high risk top priority Cyber Threats.	Tiered handling, branch/service playbooks, automation, reporting triggers
Resilience (sub-stage)	Recovery	Recovery (within CER)	Restore safely, reinforce controls, prevent recurrence, and validate return-to-service.	Safe restore gates, identity re-issue, hardening, compensating controls
Continuous Improvement	Lessons Learned	Post-Incident Activity	Convert incidents and exercises into system improvements across strategy, threat models, telemetry, detections, and playbooks.	RCA, backlog grooming, retests, purple team re-validation, model refresh

7 Engineering Extensions

1. Detection-as-Code Pipelines versioned rules with automated testing and rollback.
2. SOAR Orchestration context-driven containment and notification flows.
3. Deception Fabric honeypots and tokens collect live adversary telemetry.
4. Continuous Red/Purple Team perpetual validation of detections and response.
5. Unified Telemetry Schema consistent taxonomy across multi-cloud sources.

8 Metrics and Performance Indicators

Category	Metric	Description	Purpose
Visibility	% CJ coverage per MITRE tactic % CJ coverage per Customized Threat Modelled Data Quality Index	Telemetry depth, Coverage per crown jewel and threat model, Completeness, parsing success, latency	Ensures data relevance & usability
Detection	% of implemented and tuned detection rules per Threat Modelled % of implemented deception in each operational zone Mean Time to Detect (MTTD)	Ratio of implemented Threat modelled detection rules Time between compromise and alert, Traceability to threat model	Measures readiness & responsiveness
Response	% of implemented Response rule per detection rule Mean Time to Contain (MTTC) Mean Time to Recover/Response (MTTR)	Ratio of implemented response per detection Time from alert to containment, and resolve	Evaluates efficiency, Measures operationalization, Measures execution
Feedback	Detection Validation Rate Response readiness validation	Ratio of tested total detections rules and response playbooks (Whole IR process)	Assessment of learning loop
Strategy	% Budget linked to risk priority % of aligned process % of integration & automations % of Covered Detection per Threat Profile & TTPs	Strategic alignment Continues improvements,	Confirms governance effectiveness,

9 Industry Use Cases Samples

9.1 Cloud-Native FinTech

Vision:

- Reduce operational and systemic risk across critical payment services while maintaining availability and regulatory trust. (*Reduce Operation Risk of Payment services)

Strategy[30]:

- Adopt a threat-informed detection and response strategy focused on a high-confidence APT threat profile targeting cloud-native FinTech payment ecosystems. Prioritize adversary behaviors that impact payment integrity and identity trust boundaries.

Example[31]:

---

[30] Imagine this Banking service is Running in Europ, e.g Germany, then we can identify the potentail APT groups that targeting such and industry. Based on recent 2025 and early 2026 reports from CrowdStrike, Mandiant (Google Cloud), Trellix, and BaFin (Germany's financial regulator), the threat landscape for the German financial sector is dominated by a mix of state-sponsored APTs and highly organized eCrime groups.

Germany remains a top-tier target in Europe, suffering an estimated €267 billion in cybercrime-related losses in 2024, with that figure rising into 2025/2026.

31 trategic MITRE ATT&CK Mapping

According to the CrowdStrike 2025 European Threat Landscape Report, adversaries targeting Germany have reached record-low "breakout times" (averaging 48 minutes).

Initial Access

T1566 (Phishing): Germany is the "phishing capital" of Europe. Recent reports highlight "Quishing" (QR Code Phishing) via physical mail or fake bank notifications.

T1190 (Exploit Public-Facing Application): Massive exploitation of perimeter devices like VPN appliances (Fortinet, Ivanti) and edge routers to bypass MFA.

T1195.002 (Supply Chain Compromise): A critical 2025 trend. BaFin reports that 67% of ICT incidents in German banking originated at third-party service providers rather than the banks themselves.

Persistence & Lateral Movement

T1078 (Valid Accounts): Use of Initial Access Brokers (IABs) to buy stolen credentials. Stolen credentials rose to the second most common entry vector in 2025.

T1021.001 (Remote Desktop Protocol): Groups like Akira and RansomHub frequently use RDP for movement after gaining a foothold via compromised VPNs.

Exfiltration & Impact

T1657 (Financial Theft): Focus on Instant Payment Regulation (IPR) vulnerabilities.

T1486 (Data Encrypted for Impact): While encryption is common, 2025 saw a pivot toward Data-Only Extortion (stealing data and threatening leak without encrypting files) to avoid EDR detection.

3. Critical Regional Trends (Germany Focus)

DORA Compliance (Jan 2025): The Digital Operational Resilience Act is now fully active. German banks are reporting a spike in "ICT incidents," largely due to the new mandatory reporting requirements for supply chain failures.

Violence-as-a-Service: A chilling trend noted by CrowdStrike in late 2025 involves hybrid adversaries (like Renaissance Spider) using Telegram to coordinate physical threats against bank employees or IT staff to force credential handovers.

In the below table we consider most related APTs that potentially could target the service in this example.

Group Name	Nexus	Primary Objective	Key TTPs & Recent Activity
Lazarus Group	North Korea	Currency Generation	Targeted German crypto-exchanges and banks via AppleJeus malware and trojanized DeFi apps.
Pulsar Kitten	Iran	Espionage / Influence	Observed in mid-2025 using credential phishing targeting German industrial and transportation hubs with links to finance.
APT28 (Fancy Bear)	Russia	Geopolitical Sabotage	Active in late 2024/2025 targeting German government-affiliated financial bodies to disrupt sanctions-related data.
APT41	China	Espionage / Gain	Significant 113% increase in activity in Q1 2025; targets German financial IT supply chains to gain long-term persistence.
Scattered Spider	eCrime/Global	Financial Gain	Rapid exploitation of Okta/SSO; observed hitting European financial service providers with 24-hour "breakout" speeds.

Mapping APT & crime groups to Payment API abuse:

Actor Type	Likely API Focus
APT (espionage)	Silent access, monitoring transactions
FIN groups	Payment manipulation, laundering
Ransomware crews	Exfil + extortion via transaction data
Hacktivists	API DDoS, payment disruption

This is where APT TTPs + financial crime converge.

Crown Jewels[32]:
- Payment APIs(public and internal),
- Identity Pipelines (authN/authZ, token issuance, session lifecycle),
- Transaction processing logic and settlement workflows,
- Supporting assets: CI/CD pipelines, cloud IAM roles,
- secrets management,
- serverless workloads,
- event streams.

Visibility[33]:

AI-Driven Vishing: Voice phishing calls to German bank employees using deepfake audio of senior executives increased by over 400% in the last year.

[32] It potentially includes any critical assets that serves business operations, so in more technical level we must consider more details: e.g. DNS, related Network Services, Related containers, related Operating Systems and Applications, etc.
33 Payment API attack surface (what attackers actually go after)
Typical components:
API Gateway (REST, GraphQL)
Auth layer (OAuth2, mTLS, JWT, API keys)
Backend payment service
Integration with core banking or PSP
External consumers (apps, partners, merchants)
This maps beautifully to MITRE ATT&CK.
MITRE ATT&CK alignment to a Payment API
Initial Access
What it looks like in payments

- Threat modeling of payment and identity flows,
- Mapping to ATT&CK Cloud and Identity techniques
- Telemetry engineering: API gateway logs, serverless execution logs, IAM control-plane activity, token

Stolen API keys
Compromised OAuth tokens
Exploited API endpoint logic
MITRE
T1078 – Valid Accounts
T1550 – Use of Authentication Material
T1190 – Exploit Public-Facing Application
Payment-specific signals
Token used from new ASN / country
Sudden jump in payment initiation calls
Missing mTLS on endpoints that usually have it

Execution / Abuse
What it looks like
Abuse of legitimate endpoints
Replay of signed requests
Parameter manipulation (amount, beneficiary)
MITRE
T1204 – User Execution (API consumer acting "legit")
T1059 – Command & Scripting Interpreter (if backend abused)
T1565 – Data Manipulation
Payment signals
Same token, multiple different beneficiaries
Amount just below approval threshold
Repeated failed + successful payment attempts

Persistence (very common, very dangerous)
What it looks like
Long-lived tokens
Rogue API clients registered
Backdoor OAuth apps
MITRE
T1098 – Account Manipulation
T1136 – Create Account
T1556 – Modify Authentication Process
Payment signals
New API client with broad scopes
Token lifetime suddenly extended
Auth flows bypassing normal refresh logic

Discovery
What it looks like
Enumerating endpoints
Probing limits, currencies, accounts
MITRE
T1087 – Account Discovery
T1046 – Network Service Discovery
Payment signals
High volume of 4xx responses
Sequential account or IBAN probing
OPTIONS / schema discovery abuse

Impact (this is where money moves)
What it looks like
Fraudulent payments
Liquidity drain
Regulatory breach
MITRE
T1657 – Financial Theft
T1485 – Data Destruction (cover tracks)
Payment signals
Sudden burst of high-value transfers
Payments outside customer behavior profile
Failures in downstream reconciliation

Detection[34]:
- Privileged identity abuse and permission escalation
- API key misuse, token replay, anomalous API access
- Fraud patterns correlated with identity and API signals
- Persistence attempts via cloud configuration and identity layers,
- Characteristics: behavior-based, correlated, mapped to threat model and crown jewel risk.

Response:
- Scenario-specific playbooks aligned to crown jewels
- Automated IAM containment, session invalidation, credential revocation
- SOAR-driven fraud escalation with human decision gates for high-impact actions
- Evidence preservation and forensic readiness integrated into workflows

Sample Result: 60 % reduction in MTTR after six months, reduced blast radius for identity-related incidents, improved trust and resilience for payment services.

Note: This is a high level narrative to demonstrate the idea of the frameworks function in practice with an example. So just remember here we skipped all required details in this example and it is a high level demonstration of how to use the framework in practice. I skipped details in the example to make it simple and just demonstrate the usage concepts.

In short with knowing the main threat actors, and TTPs awe can align out Threat modelling and prioritize the high risk Threat target our environment. As a result we can have high fidelity detection rules, a more meaningful usage of threat Intelligence for threat hunting and a high readiness for response and automation response.

---

34 Detection engineering aligned to Payment API (very practical)
Core log sources you MUST have
API Gateway access logs
OAuth / IAM logs
Payment transaction logs
Backend service logs
WAF / bot protection logs
High-value detections
Token reuse across geographies
One token → many beneficiaries
Amount threshold evasion patterns
API call rate ≠ historical baseline
mTLS downgrade or missing client certs
This is ATT&CK applied to money**, not generic infra noise.**

9.2 Hybrid Bank

Vision:
- Protect financial trust and service availability by minimizing operational disruption from cyber incidents across both digital and physical banking environments.

Strategy:
- Adopt a threat-informed, crown-jewel-driven security operations model focused on rapid containment of high-impact incidents rather than broad, alert-heavy monitoring.

Crown Jewels:
- ATM network and transaction processing
- SWIFT messaging infrastructure
- Online and mobile banking platforms

These assets were prioritized based on business impact, regulatory exposure, and systemic risk.

Threat Visibility:
Engineered unified telemetry across:
- Endpoints and servers in branch environments
- Core banking and SWIFT systems
- Cloud and hybrid digital banking platforms

Telemetry was normalized and correlated to support cross-environment attack visibility rather than siloed monitoring.

Threat Detection:
Detection engineering was aligned to realistic adversary behavior, with priority coverage for:
- Credential misuse and account takeover
- Lateral movement between branch and core systems
- Remote execution and persistence techniques

Detections were mapped to MITRE ATT&CK and tuned for high-fidelity, actionable signals against crown jewels.

Response:
Implemented a tiered incident response model:
- Central SOC coordination for threat triage and decision-making
- Branch-specific playbooks enabling localized containment actions
- Clear escalation paths for incidents affecting regulated systems (e.g., SWIFT)

Response workflows emphasized speed, consistency, and business context.

Continuous Improvement:
Post-incident reviews were used to:
- Refine crown jewel prioritization
- Improve detection logic and telemetry gaps
- Update playbooks based on real incident outcomes

Possible expected Outcome:
- Mean time to contain (MTTC) reduced by **45%**
- Improved consistency of response across regional branches
- Clear alignment between security operations and business risk

9.3 OT-Heavy Manufacturer

Context:
The organization is a large industrial manufacturer with mixed legacy and modern OT environments, including programmable logic controllers (PLCs), industrial HMIs, and segmented production networks. Business risk is dominated not by data loss, but by availability, safety, and production continuity. Even short disruptions can result in financial loss, contractual penalties, and safety incidents.

The organization operates under strict constraints: no active scanning in OT, limited patching windows, and zero tolerance for response actions that could disrupt production processes.

Vision:
Ensure continuous and safe manufacturing operations by detecting and containing cyber threats targeting industrial control systems without impacting production availability or safety.
Security success was explicitly defined as preventing unplanned downtime, not maximizing alert volume or coverage metrics.

Strategy:
Adopt a threat-informed, availability-first security operations strategy focused on:
- Early detection of adversary activity targeting OT control logic and industrial protocols
- Passive visibility and behavioral detection rather than intrusive controls
- Response actions engineered to be manufacturing-safe, predictable, and reversible

The strategy intentionally avoided IT-centric SOC patterns and instead aligned detection and response design with industrial risk tolerance.

Crown Jewels:
Crown Jewels were identified through business impact analysis and operational dependency mapping:
- Production Controllers (PLCs, RTUs, Safety Controllers) Compromise could halt production lines or introduce unsafe operating conditions.
- Industrial Engineering Workstations and Logic Repositories Unauthorized modification of control logic posed long-term integrity and safety risks.
- R&D and Manufacturing Process Data Theft or manipulation could impact competitive advantage and product quality.

These assets were prioritized over peripheral IT systems, even when the latter generated more security events.

Threat Visibility (Telemetry Engineering):
Visibility was engineered outward from Crown Jewels using passive, non-intrusive methods:
- Passive OT network monitoring at key aggregation points
- Protocol-aware telemetry for:
  - Modbus
  - DNP3
  - IEC-104 (where applicable)
- Asset behavior baselining for controllers and engineering stations
- Separation of IT and OT telemetry pipelines, with correlation at the analysis layer

No active probing, vulnerability scanning, or disruptive inspection was introduced into production zones.

Outputs included:
- OT Visibility Blueprint mapped to Crown Jewels
- Known-good behavioral baselines for control traffic
- Clear telemetry gaps documented and tracked over time

Threat Detection Engineering:
Detection was engineered around behavioral deviation, not signatures or generic alerts.

Priority detection logic included:
- Anomalous command sequences sent to controllers
- Unauthorized write operations to PLC memory or logic blocks
- Protocol misuse or deviation from established communication patterns
- Engineering workstation activity outside approved maintenance windows
- Lateral movement attempts between IT and OT boundary zones

Detections were:
- Explicitly mapped to realistic OT threat scenarios
- Tuned for high confidence, even at the cost of lower coverage
- Designed to minimize false positives that could trigger unnecessary operational intervention

Detection validation relied on tabletop simulations and controlled engineering tests rather than live production testing.

Response (Manufacturing-Safe Execution):
Response workflows were engineered with availability and safety as non-negotiable constraints.

Key principles:
- No automated containment actions directly affecting controllers
- Segmentation-based containment at network boundaries
- Human-in-the-loop decision points for any action impacting production systems
- Clear coordination with OT engineers and plant operators

Response playbooks included:
- Controlled isolation of affected network segments
- Credential and access revocation for compromised engineering workstations
- Evidence preservation without system shutdown
- Safe rollback procedures aligned with maintenance windows

Response success was measured by containment without disruption, not speed alone.

Continuous Improvement (Kaizen Loop):
Each incident, anomaly, or near-miss fed a structured learning loop:
- Refinement of behavioral baselines
- Adjustment of detection thresholds
- Updates to response playbooks based on operational feedback
- Periodic validation exercises with OT and engineering teams

Continuous improvement focused on small, safe increments, avoiding disruptive changes to stable production environments.

Outcome:
After two years of operating under the UTIOM lifecycle:
- Zero unplanned production downtime caused by cyber incidents
- Improved confidence and trust between security, OT engineers, and operations
- High-fidelity detections with minimal alert fatigue
- Clear executive visibility into operational cyber risk

Most importantly, security operations were perceived as an enabler of resilience, not a threat to manufacturing stability.

Key Takeaway:
In OT environments, security operations succeed not by reacting faster, but by designing systems that respect operational reality. UTIOM enabled the organization to unify threat-informed detection, engineering discipline, and manufacturing-safe response into a single, coherent operating model.

9.4 Final example to review: Threat-Informed Operations Using Vendor Intelligence

Context:

A financial services organization operates a hybrid environment spanning on-prem core banking systems, cloud-based digital channels, and SaaS platforms. The SOC consumes multiple threat intelligence feeds but historically struggled to translate reports into actionable detection and response improvements.

A recent CrowdStrike / Mandiant / Microsoft threat intelligence report highlights increased activity by financially motivated and state-aligned actors abusing:
- Valid credentials
- Identity federation misconfigurations
- Lateral movement via remote management tooling
- Persistence through cloud and identity abuse

Rather than treating the report as "informational," the organization applies UTIOM to operationalize it.

Vision:

Ensure continued availability and trust of digital banking services by detecting and containing identity-centric intrusions before they impact regulated systems or customers.

Success is defined not by alert volume, but by time-to-detect identity abuse affecting crown jewels.

Strategy:

Based on the report, leadership agrees to:
- Prioritize identity and access abuse over malware-centric threats
- Focus detection and response effort on pre-impact attacker behavior
- Accept reduced coverage elsewhere to improve depth around critical services

This strategy explicitly deprioritizes low-risk alerts and reallocates effort toward high-impact identity attack paths.

Crown Jewels:
Using the framework, the SOC identifies:
- Cloud identity provider (IdP) and admin roles
- Online banking authentication flows
- Privileged access to payment and settlement systems

These are mapped as blast-radius amplifiers if compromised.

Threat Modeling:
The intelligence report is translated into **explicit threat models**, not narratives.
For each relevant adversary objective, **attack trees** are constructed starting from the crown jewels and expanding outward across identity, SaaS, cloud, and hybrid trust boundaries.
For the given scenario, threat modeling explores paths such as:
- Compromise of SaaS administrator accounts via phishing, MFA fatigue, or token theft
- Abuse of identity federation or trust relationships to pivot into cloud workloads
- Lateral movement from user context to privileged service and automation accounts
- Persistence through conditional access bypass, token replay, or role re-assignment

Each attack tree is analyzed to determine:
- Where controls already exist and are effective
- Where partial protection exists but is bypassable
- Where visibility is missing or insufficient
- Where detection or response would be too late to limit impact

Threat scenarios are then mapped to specific MITRE ATT&CK techniques, expected telemetry, and decision points. This produces detection stories and visibility requirements, not alerts.
The output of this stage is a coverage map that explicitly shows:
- Protected paths
- Observable paths
- Blind spots
- High-risk paths with unacceptable blast radius

This coverage map directly drives Threat Visibility Engineering, ensuring telemetry, logging, and evidence pipelines are designed to observe the highest-risk attack paths before incidents occur.

Threat Visibility Engineering:
The SOC reviews whether required evidence exists for the modeled scenarios:
- Authentication logs with token metadata
- Conditional access decision logs
- Admin API usage telemetry
- Identity role assignment changes

Gaps are identified, and telemetry pipelines are adjusted before any incident occurs.
Deception elements are added:
- Canary admin accounts
- Honeytokens embedded in privileged SaaS workflows

Threat Detection Engineering:
Detection engineers implement analytics aligned to the modeled behavior:
- Anomalous token usage across regions and services
- Privilege escalation following suspicious authentication patterns
- Admin API usage outside normal change windows

Purple team exercises emulate the reported attack paths to validate:
- Telemetry completeness
- Detection timing
- Analyst decision quality

Failed detections are treated as engineering defects, not analyst mistakes.

Threat Detection Operations:
When detections trigger:
- Alerts are enriched with crown jewel context
- Analysts assess impact, not just severity
- Identity timelines are built to confirm attacker intent

Low-context alerts are suppressed by design.

Response:
Playbooks derived from strategy are executed:
- Immediate session invalidation and token revocation
- Privilege rollback and access isolation
- Targeted communication with identity and business owners

Response authority is clear, and containment is scoped to protect critical services without unnecessary disruption.

Resilience:
Before services are fully restored:
- Identity trust relationships are reviewed
- Conditional access policies are tightened
- Detection coverage is revalidated

Restoration is gated on risk reduction, not just system uptime.

Continuous Improvement:
Post-incident or post-exercise reviews feed back into:
- Threat models (new variations observed)
- Detection logic (false positives, missed signals)
- Strategy (shift in adversary focus confirmed)

Metrics are updated to reflect real operational readiness, not tool performance.

Outcome:
- Faster detection of identity abuse
- Reduced analyst noise
- Clear linkage between threat intelligence and SOC action
- Demonstrable improvement in containment time for high-impact scenarios

Threat intelligence is no longer "read and forgotten", it becomes an input to a living operational system.

10   Outcomes and Benefits

- End-to-end traceability from strategic vision to technical execution.
- Threat-informed detection capabilities that are engineered, not assumed.
- Alignment of SOC metrics with executive expectations.
- Reduced operational noise and higher signal quality.
- A living maturity roadmap that improves itself each cycle.
- Product design and product ownership
- Economic constraints
- UTIOM operates on multiple timelines:
  - Strategic (months / years)
  - Operational (days / weeks)
  - Incident (minutes / hours)

11   Community and Governance

UTIOM is an open, living framework licensed under Creative Commons BY-SA 4.0. intended to evolve through transparent sharing and peer review.
Open Resources
- GitHub Repository documentation, examples, toolkit.
- Notion and Excel Dashboards self-assessment and scoring.
- Quarterly Kaizen Sessions community review and benchmark updates.

"Frameworks mature when communities learn together."

UTIOM aligns naturally with the NIST Cybersecurity Framework by providing an **operational execution layer** across all CSF functions.

- **Identify**
  UTIOM Vision, Strategy, and Crown Jewels directly support asset prioritization, risk understanding, and business context definition.
- **Protect**
  Strategy-driven controls and telemetry engineering inform preventive measures aligned to prioritized assets.
- **Detect**
  Threat Visibility and Threat Detection stages operationalize CSF detection outcomes through threat-informed analytics mapped to real adversary behavior.
- **Respond**
  UTIOM Response formalizes coordinated, playbook-driven incident handling consistent with CSF response planning and execution objectives.
- **Recover**
  Continuous Improvement ensures lessons learned are translated into improved posture, resilience, and operational readiness.

Key Differentiator:
While NIST CSF defines *what* good cybersecurity looks like, UTIOM defines *how to operationalize it inside a modern SOC*.

12.1 Alignment with NIST Cybersecurity Framework 2.0 (CSF 2.0)

NIST CSF 2.0 introduces GOVERN as a first-class function, emphasizing strategy, risk ownership, accountability, and outcomes. UTIOM naturally operationalizes this shift by embedding governance and decision-making directly into security operations.

GOVERN

UTIOM Vision and Strategy directly align with CSF 2.0's Govern function by:
- Defining security objectives based on business outcomes
- Establishing risk ownership through Crown Jewels identification
- Translating executive intent into operational priorities
UTIOM ensures governance is not a static policy layer but an active driver of operational behavior.

IDENTIFY

UTIOM's Crown Jewels stage fulfills CSF 2.0 Identify outcomes by:
- Prioritizing critical assets, services, and data
- Linking assets to business impact and systemic risk
- Establishing threat-informed risk context
This shifts identification from asset inventories to business-critical focus.

PROTECT

UTIOM Strategy influences Protect outcomes by:
- Guiding preventive controls toward prioritized assets
- Informing architectural decisions using threat and risk context
- Avoiding uniform control application in favor of risk-weighted protection
Protection becomes intentional and risk-driven, not checkbox-based.

DETECT

UTIOM Threat Visibility and Threat Detection directly operationalize Detect by:
- Engineering telemetry based on realistic adversary behavior
- Aligning detections to MITRE ATT&CK techniques
- Focusing on high-fidelity signals affecting Crown Jewels

Detection is treated as an engineering discipline, not alert accumulation.

RESPOND

UTIOM Response maps cleanly to CSF 2.0 Respond by:
- Enabling coordinated, role-aware response workflows
- Supporting tiered escalation and decision-making
- Embedding playbooks aligned with business and regulatory impact

Response is consistent, measurable, and context-aware.

RECOVER

UTIOM Continuous Improvement aligns with Recover by:
- Feeding incident outcomes back into strategy and detection
- Improving resilience through learning loops
- Reducing recurrence and systemic weakness

Recovery is not just restoration, but evolution of capability.

Key Insight :
NIST CSF 2.0 defines outcomes. UTIOM defines the operating model that delivers them.

13 Alignment with SOC Capability Maturity Models (SOC-CMM)

UTIOM is designed to accelerate SOC maturity progression by structuring operations around outcomes rather than tools or team silos.

- Lower maturity SOCs benefit from UTIOM's clear lifecycle and prioritization logic, reducing alert fatigue and operational chaos.
- Higher maturity SOCs leverage UTIOM to:
    - Integrate threat intelligence into detection engineering
    - Shift from reactive alerting to proactive, threat-informed operations
    - Institutionalize continuous improvement loops

UTIOM acts as a practical operating model that enables SOC-CMM capability growth across:

- People (roles, decision authority, skills)
- Process (repeatable, measurable workflows)
- Technology (telemetry, detection, automation)
- Governance (metrics, feedback, improvement)

Key Differentiator:
SOC-CMM measures *how mature a SOC is*; UTIOM provides the mechanism to become mature.

14 Alignment with the Digital Operational Resilience Act (DORA)

UTIOM directly supports DORA's objectives by embedding operational resilience into day-to-day security operations.

- ICT Risk Management
  Crown Jewels and threat-informed Strategy focus risk management efforts on systems critical to financial stability.
- Incident Detection and Response
  Threat Visibility and Detection improve early identification of systemic risks and significant incidents, enabling faster containment.
- Incident Classification and Reporting
  Tiered Response and structured playbooks support consistent incident classification, escalation, and regulatory reporting.
- Operational Resilience and Learning
  Continuous Improvement ensures operational lessons are captured and translated into improved resilience and preparedness.

Key Differentiator:
DORA mandates resilience; UTIOM operationalizes resilience through measurable, repeatable security operations aligned to real threats.

UTIOM does not replace standards or regulations. It connects them to reality.

15 Conclusion

UTIOM is a unifying language for modern defence strategic in vision, engineering in method, and human in execution. It translates intent into architecture and architecture into learning. Whether implemented in a global SOC or a two-person cloud team, the principles remain the same: define purpose, engineer detection, and learn continuously.

"UTIOM is not a just another process; it is a language that unites defenders."

UTIOM is a new approach to unified separated, siloed teams and process all into one practical and unified methodology.

"UTIOM assumes clear ownership of the security operations lifecycle, similar to product ownership in engineering organizations. Role of Security Operation Lead."

Security Operations as a Product:
UTIOM deliberately treats Security Operations and Incident Response as a product rather than a static function or reactive service. Like any well-designed product, a SOC must have a clear vision, an evolving strategy, engineered features, measurable outcomes, and continuous feedback from real-world usage. This mindset shifts the focus from operating tools and managing alerts to delivering consistent risk reduction, resilience, and business value. In UTIOM, improvement is not an initiative; it is the product lifecycle itself.

Security operations will not mature by adding more tools.
They mature when treated as a system, designed with intent, and improved deliberately.

About the Author

Who am I?

Reza Adineh is a German-based cybersecurity architect and visionary with over 15 years of experience designing and leading Security Operations Centres across banking, cloud, and hybrid environments. After years of building & Operating SOCs, realized that true resilience doesn't come from technology alone it comes from unifying strategy, engineering, and continuous learning. From that vision, UTIOM was born. As creator of the STRATA and TID-CMM frameworks and founder of Minimal Cyber, focuses on transforming detection and response into intelligent, adaptive systems that connect purpose, people, and precision.

---

i The V-Model is a procedural model that visually demonstrates the relationship between each stage of the development life cycle and its corresponding testing phase, which creates the "V" shape.

Left Side (Verification/Development Phases): The process moves downward from high-level, abstract requirements to detailed design specifications. This phase ensures you are "building the product right" according to the plan.

Right Side (Validation/Testing Phases): The process moves upward, involving testing activities that correspond directly to a development phase on the left. This phase ensures you are "building the right product" that meets the user's actual needs.

The Bottom of the V: Represents the coding or implementation phase, where the actual product is built.

IAPM - International Association of Project Managers

Requirements Traceability in the V-Model

Requirements traceability is the ability to track the life of a requirement from its origin through development and testing back to its source or vice versa.

Purpose: It ensures that every single requirement defined at the beginning of the project is accounted for, implemented, and thoroughly tested.

Mechanism: Traceability links connect requirements documents (left side) to their relevant test cases (right side). For example, the initial user requirements are linked to the User Acceptance Tests (UAT).

Benefit: This clear, bidirectional link makes it easier to track progress, manage changes, ensure quality and compliance (especially in safety-critical industries like automotive or medical devices), and prevent overlooked requirements.

ii With having the threat profiling, knowing targeted high risk threats, having threat modelling and related threat detection rules, leveraging threat intelligence, we can work on threat hunting with a clear strategy of what we should looking for. Furthermore, in order to improve our threat detection program we can use the OODA loop, in order to see how effective is our current detection rules. For testing the rules, using Purple teaming, Red teaming is the way to go.

Knowing threat detections, we can now think of response plan and if possible business continuity plan based on realistic threats we already monitoring. It could lead to asset reclassification as well.

This is the last step of our main steps, continues improvement. With continues improvements we will take a look to the whole cycle, and see how and where we can improve. And this could lead to refine the strategies.

iii UTIOM complements, not replaces, all mapped frameworks.

iv from Sun Tzu's The Art of War :"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Key Takeaways from the Text

Sun Tzu doesn't just mention "strengths and weaknesses" in passing; he dedicates an entire chapter (Chapter 6: Weak Points and Strong) to how you should apply that knowledge.

Self-Knowledge: This is about "knowing yourself"—understanding your own resources, morale, and limitations.

In cyber security, applying Sun Tzu via a SWOT lens means moving from reactive "firefighting" to proactive defense. Knowing yourself involves rigorous asset discovery and vulnerability management—identifying your "Weaknesses" (unpatched software) and "Strengths" (i.g.,robust encryption). Knowing the enemy means utilizing Threat Intelligence to understand the "Threats" (specific hacker groups/TTPs) and "Opportunities" (gaps in the attacker's own infrastructure). By aligning these, a CISO ensures that security controls aren't just a wall, but a strategic maneuver that makes the cost of an attack higher than the potential reward.

v https://www.linkedin.com/pulse/from-ppt-strata-reza-adineh-ysqhf/?trackingId=%2FkSuK87cQRGkLDSGcxcCsw%3D%3D

vi Threat Informed Detection Capability Maturity Model